Air Force Office for Security Review
Web Site Review Checklist

This checklist is an adaptation of AFI 33-129, AFI 35-101, and the SAF/PAS Security Review Guide. It is designed to assist reviewers in conducting a Web review of their public Web site. All Air Force agencies have been directed to conduct an annual review of public Web sites to ensure that it does not contain sensitive information. The intention is not to remove or deny public access to Air Force information, but to prevent inadvertent or unauthorized public release of sensitive information via the Web. Placing material on a public Web site constitutes global public release and makes information immediately available for aggregation and electronic manipulation via data mining. A Web review ensures that the American public is served without jeopardizing military operations or personnel. The Air Force has more than 160,000 known Web pages to review.

The following are standard points we use in evaluating suitability for approval of all sites and web information submitted for security and policy review.

Availability. Material submitted for review should not already be in the public domain. Material in the public domain can be of two types: Common domain information (previously released, previously cleared, basic scientific research under no intellectual property restrictions, or publicly available) or inadvertently released.

Common domain information. No need to review this information. Posting of information still requires a common sense test of basic standards.

Inadvertent release information.

a. If information passes the tests involved in paragraph 4, then we have no objection to its continued release.

b. If information does not pass the tests involved with paragraph 4, then the material must be removed from public access, because it conflicts with official policy.

c. Inadvertent releases point out information security weaknesses which must be addressed. Leaks through bad web controls must be rectified, leaks through bad security and policy review procedures must be handled.

Information Content. Information should pass the standard tests of a good security review program.

Neighborhood. The path to the site should not also have branches which could lead to controversial, inappropriate web sites.

Links.

a. Links to other sites should not convey AF endorsement.

b. Web master should establish a non-discriminatory policy with regard to links. That is: A link to product A is placed on the site. Product B is just as useful to the user as product A. The webmaster should then link also to Product B.

c. Links are not permitted to controversial, inappropriate web sites.

Warning notices.

a. Monitoring notice. DOD computer systems are provided for the processing of official U.S. Government information only. The system is monitored to ensure information security, system integrity, and the limitation of use to official purposes. Your use of this system is subject to monitoring at all times. Unauthorized or illegal activities, involving this system, can result in criminal prosecution under the Computer Fraud and Abuse Act of 1986.

b. Intellectual property notice. Users may use all information freely. OR Please contact the webmaster for reuse of the following items of information.

c. Non Endorsement notice. Reference to the following items does not constitute official Air Force endorsement of the organizations or their products.

d. Linking notice. Webmaster is not responsible for the content and accuracy of information contained in links outside my domain.

CHECKLIST

Is Web site a public site with no access restrictions?

ð__URL address of site: (i.e. www.af.mil) _____

ð__ POC of site or site administrator: _____
(Name, phone)

ð__Proper public Web site disclaimer

2. Is the web site registered with Air Force Link?
   ð Yes. If not, the site should be access controlled until reviewed (AFI 35-101) and registered.

3. Has an initial Security and Policy Review been conducted
   ð__Date: _____ Case Number: _____

4. Does the site contain sensitive information? (please indicate page URL)
   ð__Classified or FOUO data
   ð__FOIA exempt data
   ð__Lessons learned or analysis of sensitive military operations or vulnerabilities
   ð__Sensitive movement, unit locations or installations or plans
   ð__Personal information (sensitive positions, routinely deployable units)
   ð__Privacy Act data (birthdate, SSN, home address, home phone)
   ð__Family member personal data
   ð__Contractor Proprietary Information
   ð__Test and Evaluation data
   ð__Technical information not marked for distribution "A."

5. Are copyrighted materials used on the page (text or graphics)?
   ð__Corporate logos, software graphics
   ð__Other: _____

6. Are there product endorsements links to commercial sites that may imply endorsement?
    - ð__Yes, but they are mission related.
    - ð__Links are to commercial software (no logos)
    - ð__Is a specific browser or software recommended?
    - ð__External framing used.
    - ð__Links to restricted sites (single link to logon screen is proper)

7. Does the site contain W3C nonstandard plugins, executables or files:
    - ð__Microsoft Word, Excel files
    - ð__ ActiveX or Frontpage bots
    - ð__Zip or self-expanding (exe) files

8. Does the site contain Non-OMB approved surveys or questionnaires?

The following is a list of materials that are not recommended for posting on Air Force Public Web pages and may violate InfoSEC or OPSEC concerns. * *Indicates likely FOUO*.

Military Operations & Exercises information relating to:

- Unit Organization
- Unit readiness specific
- Detailed mission statement
- Specific Unit phone/fax numbers (secure and unsecured)
- Time-Phase Force Deployment Data (TPFDD)
- Ops schedules
- Logistics support requirements
    - Medical
    - Civil engineering
    - POL
    - Host nation support
    - Transportation
    - Munitions
- Force Apportionment
- Force Allocation
- Unit Beddown information
- Planning guidance
- Unit augmentation
- Force Synchronization
    - Unit shortfalls
- Counter-terrorism information
- Detailed Budget Reports
- Images of Command and Control (C2) nodes
- Inventory reports
- Intelligence, Surveillance and Reconnaissance (ISR) Capabilities
- Command, Control, Communications, Computers and Intelligence (C4I) Architecture
- Non-Combatant Evacuation Operations (NEO) Plans or Ops

- Counter-drugs Ops
- Unit Recall Rosters
- Weapons Movements
- Mobilization information
- Detailed maps or installation photography
- Standard Operating Procedures
- Tactics, Techniques, and Procedures
- Critical maintenance

Personnel information relating to:

• Information, the release of which would be a clearly unwarranted invasion of personal privacy, to include the following categories about U.S. citizens, DoD employees and military personnel:

- Social Security Account Numbers; 2) dates of birth; 3) home addresses, and 4) telephone numbers other than duty office numbers. Duty phone numbers of units described in C.3.2.1.6.2.2. of DoD 5400.7-R (reference (j)) may not be posted.*
- Names, locations, and any other identifying information about family members of DoD employees and military personnel*
- Official travel itineraries of individuals and units before it is performed*
- Duty rosters, or detailed organizational charts and directories with names (as opposed to Organizational charts, directories, general telephone numbers for commonly requested resources, services and contacts without names)*
- Internal DoD personnel rule and practice unless cleared for release to the public*
- Financial Disclosure Reports of Special Government Employees (5 USC App. 4, §207 (a) (1) (2)*
- Representation Rights and Duties, Labor Unions (5 USC §7114 (b)(4))*
- Action on reports of Selection Boards (10 USC §618)*
- Confidential Medical Records (10 USC §1102)*
- Civil Service Examination (18 USC §1917)*
- Drug Abuse Prevention/Rehabilitation Records (21 USC §1175)*
- Confidential of Patient Records (42 USC §290dd-2)*
- Information Concerning US Personnel Classified as POW/MIA during Vietnam Conflict (42 USC §401)*
- Information Identifying Employees of DIA, NRO, and NIMA (10 USC §424)*

Proprietary Information submitted by a contractor and protected by a Limited Rights Statement or other agreement, and trade secrets, commercial and financial information submitted by an entity outside the government that considers the information to be protected from release to the public. Other specific provisions include:

- Contractor Proposals (10 USC §2305 (g))*
- Commercial or financial information received in confidence with loans, bids, contracts or proposals*
- Information received in confidence e.g. trade secrets, inventions, discoveries or other proprietary data*
- Statistical data and commercial or financial information concerning contract performance, income, profits, losses and expenditures, if offered and received in confidence from a contractor or potential contractor*

- Scientific and manufacturing processes or developments concerning technical or scientific data and other information submitted with an application for research grant or with a report while research is in progress*
- Test and evaluation of commercial products or military hardware produced by a non-governmental entity*
- Patents, unless licensed for publication by the United States*
- Software documentation: shall be distributed according to the terms of the software license*
- Premature Dissemination: The information related to patentable military systems or processes in the developmental stage.*
- Confidential Status of Patent Applications (35 USC §122)*
  - Secrecy of Certain Inventions and Withholding of Patents (35 USC §181-188)*
  - Confidential Inventions Information (35 USC §205)*

Test and Evaluation information could result in an unfair advantage or disadvantage to the manufacturer or producer or could reveal the capabilities, limitations, or incapability's of a DoD weapons systems or component.

Scientific and technological information relating to:

- Critical technology on either the Munitions List or the Commerce Control List*
- Unclassified Special Nuclear Weapons Information (10 USC §128)*
- Unclassified Technical Data with Military or Space Application (10 USC §130)*
- Centers for Industrial Technology – Reports of Technology Innovations (15 USC §3705 (e)(E))*
- Information Regarding Atomic Energy (42 USC §2161-2168)*
- Control of Arms Exports Sec 38(e) of the Arms Export Control Act (22 USC §2778(e))*
- Technical and scientific data developed by a contractor or sub-contractor exclusively or in part at private expense*
- Sensitive S&T Reports such as:*
  - Defense Acquisition Executive System Reports
  - Selected Acquisition Reports
  - Weapons System Unit Cost Reports
  - Approved Program Baselines for ACAT I, II, III Weapons Systems
  - Weapons Systems Evaluation and Testing Results and Reports
  - Reports Based on Joint USA and Foreign Government Technical Research and Weapons Systems Evaluations
  - Weapons System Contractor Performance Reporting Under earned Value Reporting System at the Level of CPE Reporting
  - Weapons Systems staff working papers, correspondence and staff assessments
  - DoD Component "Feedback" staff working papers and assessments on weapons System Program Performance

Intelligence information relating to:

- Organizational & Personnel Information for DIA, NRO and NIMA (10 USC §424)*
- Maps, Charts, and Geodetic Data (10 USC §455)*
- Communications Intelligence (18 USC §798)*
- NSA Functions and Information (50 USC §402)*
- Protection of Identities of US Undercover Intelligence Officers, Agents, Informants and

Sources (50 USC §421)*
- Protection of Intelligence Sources and Methods 50 USC §403(d)(3))*

Other information relating to:
- A-76 studies and other outsourcing studies that provide detailed descriptions of sensitive organizational operations
- Administrative Dispute Resolutions (5 USC §574 (j))*
- Confidentiality of Financial records (12 USC §3403)*
- National Historic Preservation (16 USC §470w-3)*
- Internal advice, recommendations and subjective evaluations*